Sujet de thèse - Chemins d'attaques dans les architectures hyper connectées : de la modélisation au renforcement de la résilience; de l'analyse post-mortem à la reconstruction

L'Institut de Recherche Technologique (IRT) System X a pour ambition de devenir une référence mondiale dans le domaine de l'ingénierie numérique. Pour cela, il s'appuie sur la co-localisation des ressources à la fois industrielles et académiques lui permettant d'avoir une efficacité et une dynamique d'innovation. Cette dernière favorise le décloisonnement des mondes publics et privés en abordant des thématiques de R&D prometteuses et des sujets de recherche d'avenir.

DÉFINITION DU CADRE DE LA THÈSE

Intégré au sein de l'Institut de Recherche Technologique System X, situé à Saclay et en étroite collaboration avec des industriels et des académiques, vous êtes amené à prendre part et à contribuer au rayonnement scientifique de System X. Vous travaillerez dans un environnement stimulant avec les meilleurs laboratoires de recherche Français (Inria, CEA, Institut Mines-Télécom, UP11, UTT (Troyes), UVSQ,…) et en étroite collaboration, sur des projets scientifiques prometteurs, avec des industriels (Airbus Group, Gemalto, GDF Suez, …).

DESCRIPTIF DU SUJET de RECHERCHE

Le projet EIC (Environnement d'Intégration et d'Interopérabilité en Cybersécurité) vise à mettre en œuvre une plateforme expérimentale et technique en cybersécurité appelée CHESS (Cybersecurity Hardening Environment for Systems of Systems) qui permettra d'évaluer le couplage de technologies de cybersécurité à travers des cas d'usage innovants dans le domaine des SmartGrids, de l'Usine du Futur, du Transport Connecté et Autonome et des nouveaux services de l'Internet des Objets.
Dans cette thèse, on cherche à mettre en place de nouvelles solutions et de développer des outils facilitant l'analyse et la compréhension des chemins d'attaques redoutés ainsi que les autopsies mortem ou post-incidents sur les cas d'usage du projet EIC. Trois étapes pourront être franchies :

1/ État de l'art sur les modèles de chemins d'attaque existant sur les architectures IT « classiques ».
Ces modèles nécessitent des outils de corrélation d'évènements qui ont pour but de croiser plusieurs indices et évènements provenant de plusieurs sources et ainsi d'arriver à remonter le fil des attaques et incidents de sécurité. Il s'agit, pour cela, de réduire le grand nombre d'alertes levées ainsi de réaliser des tâches d'analyse de haut niveau pour une meilleure compréhension des scénarios d'attaques et une anticipation des plans d'actions jusqu'à l'étude d'impacts.

2/ Modèle théorique sur les architectures hyper connectées.
Un modèle théorique de chemins d'attaques sera proposé s'appliquant aux architectures nouvelles sur les cas d'usage cités ci-dessus, soit à partir de l'adaptation d'une méthode existante, soit à partir de concepts novateurs. Un verrou scientifique, ouvert dans cette thèse, correspond donc à améliorer les modèles de génération de graphes d'attaques, voire d'en proposer un nouveau pour la détection d'intrusion et l'identification d'attaques réseaux.
Les outils de modélisation-utilisés pour la reconstitution de scénarios d'attaques proviennent assez souvent des études de fiabilité comme les arbres de défaillance, graphes d'attaques, modélisation des systèmes complexes, etc. Néanmoins, ces outils présentent l'inconvénient d'être statiques. Le caractère dynamique nécessite des approches comme la modélisation d'attaques par réseaux de Petri, les *goal-inducing attack chains*, les réseaux bayésiens, etc.

3/ Mise en œuvre du modèle théorique, au moins sur des architectures IT « classiques »
La validation du modèle se fera sur des architectures tests qui seront mises en place dans la plateforme du projet EIC à l'IRT SystemX sur laquelle seront simulés des scénarios d'attaques rejouables. L'évaluation de sa pertinence s'appuiera sur les traces collectées via ces nouveaux systèmes hétérogènes qui requièrent des algorithmes efficaces pour trouver des associations entre elles.

COMPÉTENCES REQUISES

- Maîtrise de langages de programmation : Java, C++ ou Python ;
- Connaissances en mathématiques appliquées : probabilité, algèbre, etc. ;
- Capacité à appréhender rapidement des architectures de SI complexes (OS, réseau et connectivité radio, middleware, base de données SQL/NoSQL, etc.)

APTITUDES PERSONNELLES

- Personne communicante et dynamique ;
- Autonome et bon esprit d'initiative

LOCALISATION ET CONTACTS

Ref : Thèse-EIC-2

Localisation: IRT System X, 8 Avenue de la Vauve, 91120, Palaiseau.

Contacts: Philippe Wolf : philippe.wolf@irt-systemx.fr
Patrick Lallement : patrick.lallement@utt.fr
Makhlouf Hadji: makhlouf.hadji@irt-systemx.fr